

TIMOTHY R. TITOLO, ESQ.  
Nevada Bar No. 3617  
TITOLO LAW OFFICE  
9950 West Cheyenne Avenue  
Las Vegas, Nevada 89129  
Phone: (702) 869-5100  
Email: tim@titololaw.com

*Attorney for Plaintiffs PETER DELVECCHIA & A.D., A MINOR*

CHARLES A. MICHALEK, ESQ.  
Nevada Bar No. 5721  
ROGERS, MASTRANGELO, CARVALHO & MITCHELL  
700 South Third Street  
Las Vegas, Nevada 89101  
Phone: (702) 383-3400  
Email: [cmichalek@rmcmlaw.com](mailto:cmichalek@rmcmlaw.com)

*Attorneys for Defendants*

UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA

PETER DELVECCHIA, individually and as  
next friend of A.D., a Minor,

*Plaintiffs,*

v.

FRONTIER AIRLINES, INC., et al.,

*Defendants.*

Case No.: 2:19-cv-01322-KJD-DJA

**STIPULATED [PROPOSED]  
PROTECTIVE ORDER  
REGARDING SENSITIVE SECURITY  
INFORMATION**

**STIPULATED PROTECTIVE ORDER GOVERNING ACCESS TO, HANDLING OF, AND  
DISPOSITION OF POTENTIAL SENSITIVE SECURITY INFORMATION**

In accordance with Section 525(d) of the Department of Homeland Security Appropriations Act, 2007, Public Law No. 109-295, § 525(d), 120 Stat. 1382, 1355 (Oct. 4, 2006), as reenacted (the “Act”), and further in accordance with the Court’s April 1, 2020 Order (ECF No. 76) designating Plaintiff Peter DelVecchia and his attorney John D. McKay as “Covered Persons” under the Act, the Court hereby enters this Protective Order Governing Access to, Handling of, and Disposition of Potential Sensitive Security Information (the “Order”) exchanged in the above-captioned matter (this “Litigation”).

1     **1.     Scope**

2             1.1     This Order shall govern any Document, information or other material that contains  
3     “Sensitive Security Information” as defined herein, including Documents containing Sensitive Security  
4     Information that are produced by the Parties, Documents produced by non-parties, and Documents  
5     produced by government agencies. Any Party serving a subpoena or other request for information or  
6     materials (including a request to a government agency made pursuant to 5 U.S.C. § 301) upon a non-  
7     party or a government agency shall serve a copy of this Order along with the subpoena or other request.

8             1.2     Nothing contained herein alters or affects in any manner a covered person’s obligations  
9     and duties as set forth in 49 C.F.R. Part 1520.  
10

11     **2.     Definitions**

12             2.1     Court Designated Covered Person. The term “Court Designated Covered Person” shall  
13     refer to Plaintiff Peter DelVecchia and his attorney, John D. McKay, who are not otherwise authorized  
14     to have access to Sensitive Security Information in the course of this litigation pursuant to 49 C.F.R. Part  
15     1520, but who the Court has cleared for access to relevant Sensitive Security Information after  
16     determining that (a) each has a substantial need for relevant Sensitive Security Information in the  
17     preparation of this case, (b) each is unable without undue hardship to obtain the substantial equivalent of  
18     the relevant Sensitive Security Information by other means, and for whom TSA has determined that (c)  
19     such access does not present a risk of harm to the nation based upon a criminal history records check,  
20     terrorist threat assessment, and evaluation of the sensitivity of the information as mandated by Section  
21     525(d) of the Act.  
22

23             2.2     Statutory Covered Person. The term “Statutory Covered Person” shall refer to Defendant  
24     Frontier Airlines, its counsel, and legal support staff working under counsel’s supervision, who are  
25  
26  
27  
28

1 authorized to have access to specific Sensitive Security Information pursuant to 49 C.F.R § 1520.7 and  
2 1520.11.

3 2.3 Documents. The term “Documents” shall include, but is not limited to, all written  
4 or printed matter of any kind, formal or informal, including originals, conforming and non-conforming  
5 copies (whether different from the original by reason of notation made on such copies or otherwise).  
6

7 The term further includes, but is not limited to, the following:

8 a. papers, correspondence, memoranda, notes, letters, reports, summaries, photographs,  
9 maps, charts, graphs, inter-office and intra-office communications, notations of any sort concerning  
10 conversations, meetings, or other communications, bulletins, teletypes, telegrams, telefacsimiles,  
11 invoices, worksheets, transcripts of any kind (including depositions and Court proceedings), legal briefs,  
12 pleadings and papers (including those filed with the Court) and drafts, alterations, modifications,  
13 changes and amendments of any kind to the foregoing;  
14

15 b. graphic or oral records or representations of any kind, including, but not limited to,  
16 photographs, charts, graphs, microfiche, microfilm, videotapes, sound recordings of any kind, and  
17 motion pictures;  
18

19 c. electronic, mechanical or electric records of any kind, including, but not limited to,  
20 tapes, cassettes, disks, recordings, electronic mail, films, typewriter ribbons, word processing or other  
21 computer tapes or disks, and all manner of electronic data processing storage.

22 2.4 Restricted Use Document. The term “Restricted Use Document” shall refer to any  
23 Document that contains Sensitive Security Information.  
24

25 2.5 Parties. The terms “Party” and “Parties” refer to the parties to this Litigation and their  
26 counsel as well as any and all future parties to this Litigation.  
27  
28

1           2.6    Sensitive Security Information. The term “Sensitive Security Information” shall have the  
2 meaning set forth in 49 U.S.C. § 114(r)(1)(C), 49 C.F.R. § 1520.1 et seq., and as designated in orders  
3 issued by TSA pursuant to 49 U.S.C. § 114(r).  
4

5           **3.       Identification and Review of Sensitive Security Information**

6           3.1    All Documents sought to be produced or otherwise exchanged in connection with this  
7 Litigation that contain, or that the producing party has reason to believe contain, Sensitive Security  
8 Information, shall first be submitted to TSA for review, with an accompanying index of the submitted  
9 Documents, as required under 49 C.F.R. § 1520.9(a)(3), EXCEPT THAT Documents in Frontier’s  
10 custody, possession or control that discuss Threat Levels and training concerning Threat Levels and  
11 physical contact with passengers have already been cleared by TSA for production to Peter DelVecchia  
12 and John D. McKay without redaction and shall be so produced immediately upon entry of this Order.  
13

14           3.2    TSA shall promptly complete a review to determine if any particular Document  
15 submitted contains Sensitive Security Information. Upon completion of this review, to the extent that a  
16 Document does not contain Sensitive Security Information, TSA shall authorize the release of the  
17 Document and the Document shall no longer be subject to this Order. Information that TSA has  
18 determined does not constitute Sensitive Security Information may be used and disclosed in any manner  
19 consistent with the disclosure procedures governing non-Restricted Use Documents exchanged in this  
20 Litigation.  
21

22           3.3    Upon completion of this review, to the extent that TSA determines that a Document does  
23 contain Sensitive Security Information, TSA shall redact the specific Sensitive Security Information  
24 from the face of the Document and provide such redacted version to the entity that submitted the  
25 Document for review. TSA shall authorize the production of such Documents as redacted and such  
26  
27  
28

1 redacted Documents may be used and disclosed in any manner consistent with the disclosure of non-  
2 Restricted Use Documents exchanged in this Litigation.

3           3.4     Should it come to TSA's attention that it may have inadvertently failed to designate  
4 material as Sensitive Security Information, TSA may review any Document to reassess whether it  
5 contains any Sensitive Security Information. To the extent that TSA determines upon re-review that the  
6 Document does not contain any Sensitive Security Information, TSA shall authorize the Document for  
7 production pursuant to Section 3.2. of this Order; to the extent TSA determines upon re-review that the  
8 Document does contain Sensitive Security Information, TSA shall apply the procedures of Section 3.3 of  
9 this Order and require that any Court Designated Covered Person or Statutory Covered Person, who  
10 does not otherwise have a right to access that Sensitive Security Information independent of this  
11 Litigation, immediately submit written certification to TSA that all unredacted copies of the Document  
12 have been destroyed.

15 **4.     Access to Sensitive Security Information**

16           4.1     Access to the Sensitive Security Information under the terms and conditions of this Order  
17 shall be restricted to:

- 18                   a.     Statutory Covered Persons;
- 19                   b.     Court Designated Covered Persons in accordance with Section 4.2 of this Order;
- 20                   and
- 21                   c.     Designated court personnel and court reporters (including videographers) who have
- 22                   signed EXHIBIT A.

23           4.2     If a Court Designated Covered Person seeks access to the Sensitive Security Information  
24 contained in any Restricted Use Document, provided that TSA and the Court have determined that Court  
25 Designated Covered Person has a substantial need for relevant Sensitive Security Information in the  
26  
27  
28

1 preparation of this case, and is unable without undue hardship to obtain the substantial equivalent of the  
2 relevant Sensitive Security Information by other means, TSA will grant Court Designated Covered  
3 Person access to the specific Sensitive Security Information, unless TSA determines that such access  
4 would present a risk of harm to the nation.  
5

6 4.3 If TSA determines that it is appropriate to grant Court Designated Covered Person access  
7 to specific Sensitive Security Information pursuant to Section 4.2 of this Order, it will authorize  
8 production to the requesting Court Designated Covered Person of a Restricted Use Document with the  
9 specific Sensitive Security Information unredacted.  
10

11 4.4 To the extent that a Restricted Use Document contains a range of Sensitive Security  
12 Information, some of which TSA determines is appropriate for production to Court Designated Covered  
13 Person and some of which is inappropriate for production under the criteria set forth in Section 4.2 of  
14 this Order and Section 525(d) of the Act, TSA shall redact the Sensitive Security Information that is  
15 inappropriate for production. TSA shall then authorize the production of such Restricted Use Document  
16 to Court Designated Covered Person only in such redacted form.  
17

18 4.5 Should attorney John D. McKay cease representing the Plaintiffs in this Litigation, for  
19 whatever reason, such Court Designated Covered Person shall no longer be cleared for access to  
20 Sensitive Security Information. Plaintiffs may elect to have a new attorney undergo the vetting process  
21 described in Section 525(d) of the Act in order to obtain access to Sensitive Security Information in this  
22 Litigation.  
23

24 4.6 In the event that Court Designated Covered Person loses or relinquishes his or her  
25 clearance for access to Sensitive Security Information, for whatever reason, the former Court Designated  
26 Covered Person must promptly certify in writing to TSA that all Sensitive Security Information in his or  
27  
28

her custody has been destroyed or that all Sensitive Security Information in his or her custody has been transferred to the new Court Designated Covered Person in this Litigation.

4.7 All Restricted Use Documents subject to this Order in the possession Court Designated Covered Person employees of Court Designated Covered Person, and party-designated consultants and experts shall be certified in writing to have been destroyed within 60 days of termination of this Litigation, including any appellate proceedings.

**5. Non-Disclosure of Sensitive Security Information**

5.1 Except as provided in this Order, persons authorized to have access to Sensitive Security Information pursuant to 4.1 of this Order are prohibited from disclosing, in any manner, or otherwise providing access to, Sensitive Security Information, however obtained, to any individual or entity.

5.2 Except as provided in this Order, persons authorized to have access to Sensitive Security Information pursuant to Section 4.1 of this Order are prohibited from aiding or assisting any person or entity in disclosing, in any manner, or otherwise providing access to, Sensitive Security Information.

5.3 Litigation support staff, including paralegals and administrative assistants, and expert consultants and witnesses may not be granted access to Sensitive Security Information unless specifically authorized by this Order or by TSA in writing.

5.4 Any authorized disclosure of Sensitive Security Information must be made pursuant to Sections 6, 7, and 8.

**6. Production of Documents**

6.1 Prior to production, the entity responsible for producing Restricted Use Documents shall label or stamp any such Document with the following language:

**SUBJECT TO SENSITIVE SECURITY INFORMATION PROTECTIVE ORDER  
IN DELVECCHIA V. FRONTIER AIRLINES, CIVIL ACTION NO. 19-CV-  
01322 (DISTRICT OF NEVADA) SENSITIVE SECURITY INFORMATION**

1       **WARNING: THIS RECORD MAY CONTAIN SENSITIVE SECURITY**  
2       **INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 1520. NO**  
3       **PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A**  
4       **'NEED TO KNOW,' AS DEFINED IN 49 CFR PART 1520, EXCEPT WITH THE**  
5       **WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE**  
6       **TRANSPORTATION SECURITY ADMINISTRATION. UNAUTHORIZED**  
7       **RELEASE MAY RESULT IN CIVIL PENALTY OR OTHER ACTION.**

8       6.2     All Restricted Use Documents shall be produced either in hardcopy or on a password  
9       protected disk by mail, courier, or overnight delivery service, or by creating password-protected  
10      electronic files and transmitting via email. Passwords should be shared only with persons enumerated in  
11      section 4.1 of this order and, must not be sent via the same package or in the same electronic message  
12      containing Restricted Use Document attachments.

13      6.3     Only persons authorized to have access to SSI pursuant to Paragraph 4.1 of this Order  
14      may maintain custody of Restricted Use Document(s), and such persons have a duty to safeguard the  
15      Restricted Use Document(s) and the SSI contained therein, from unauthorized disclosure. When not in  
16      the physical possession of such persons, the hardcopies of Restricted Use Document(s) shall be stored in  
17      a secured container, such as a locked desk or file cabinet.

18      6.4     Persons authorized to have access to Sensitive Security Information pursuant to Section  
19      4.1 of this Order may create Documents containing Sensitive Security Information found in a Restricted  
20      Use Document, provided that any such Document is secured in the same or equivalent manner, to the  
21      same or equivalent extent, and with the same restrictions on access as set forth in this Section 6.

22      **7.     Use of Sensitive Security Information in Depositions and Examinations**

23      7.1     Sensitive Security Information that is authorized for production pursuant to Section 4 of  
24      this Order may be used and/or elicited during the deposition or examination of a witness, provided such  
25      witness is a Covered Person, subject to the following restrictions:  
26  
27  
28



1           7.1.1 Only the individuals identified in Section 4.1 of this Order may be present in the  
2 room when such Sensitive Security Information is used and/or elicited.

3           7.1.2 To the extent that attorney John D. McKay or a Covered Person wishes to use a  
4 Restricted Use Document as an exhibit at a deposition, Mr. McKay or a Covered Person may print a  
5 limited number of hard copies of such Restricted Use Document using a secure printer located at Mr.  
6 McKay's or the Covered Person's place of employment for use solely as exhibits at the deposition,  
7 provided that at the conclusion of the deposition, the original marked deposition exhibit and all hard  
8 copies are collected and maintained by a court reporter authorized to have access to Sensitive Security  
9 Information in accordance with Section 4.1(c) of this Order. The court reporter shall secure the  
10 Restricted Use Documents in the same manner, to the same extent, and with the same restrictions on  
11 access prescribed in Section 6 of this Order.  
12

13           7.1.3 Sensitive Security Information that is not authorized for release pursuant to  
14 Section 4 of this Order may not be used or elicited during the examination of a witness.  
15

16           7.2 The court reporter who records a deposition shall promptly submit the deposition  
17 transcript to TSA for review. TSA shall promptly complete a review to determine if a deposition  
18 transcript contains Sensitive Security Information. To the extent that TSA determines, upon review of  
19 the deposition transcript, that the transcript contains Sensitive Security Information that is appropriate  
20 for release pursuant to Section 4 of this Order, TSA shall authorize the transcript for release to counsel  
21 for Covered Persons and to Court Designated Covered Person with all such appropriate Sensitive  
22 Security Information unredacted from the transcript.  
23

24  
25 **8. Use of Sensitive Security Information in Motions and Court Proceedings**

26           8.1 Any Party who wishes to use a Restricted Use Document or the Sensitive Security  
27 Information contained therein in connection with a motion or other submission to this Court must file  
28

1 the Restricted Use Document and any pleadings, motions or other papers containing Sensitive Security  
2 Information under seal. Where possible, only the portions of the filings that contain Sensitive Security  
3 Information shall be filed under seal.

4  
5 8.2 All court proceedings, or portions thereof, in which Sensitive Security Information may  
6 be disclosed, shall be closed to the public. If there is a possibility that Sensitive Security Information  
7 may be disclosed during any portion of the trial, such as the testimony of a particular witness, the  
8 courtroom shall be closed to the public for that portion.

9 **9. Dispute Resolution**

10  
11 9.1 To the extent there is a dispute between the Parties concerning whether information  
12 constitutes Sensitive Security Information, the Party raising the dispute shall refer the matter to TSA for  
13 a determination by the close of discovery. If a Party does not agree with TSA's determination it shall  
14 request in writing that TSA issue a final order pursuant to 49 U.S.C. § 114(r) designating such  
15 information as Sensitive Security Information. TSA final orders concerning the designation of  
16 information as Sensitive Security Information are reviewable exclusively in the United States Court of  
17 Appeals in accordance with 49 U.S.C. § 46110.

18  
19 9.2 To the extent there is a dispute concerning whether specific redacted or withheld  
20 Sensitive Security Information should be authorized for production under Section 4 of this Order and  
21 Section 525(d) of the Act, the Parties shall meet and confer in an attempt to resolve the dispute  
22 consensually. For all unresolved disputes concerning whether specific Sensitive Security Information  
23 should be authorized for production, a Party (or Parties) may submit the dispute to the Court.

24  
25 9.2.1 TSA final orders concerning whether a risk of harm to the nation is presented by  
26 granting access to specific Sensitive Security Information, either because of the sensitivity of the  
27 information or the results of the criminal history records check and terrorist threat assessment as set  
28

1 forth in Section 525(d) of the Act, are reviewable exclusively by the Court of Appeals in accordance  
2 with 49 U.S.C. § 46110.

3 **10. Unauthorized Disclosures**

4 10.1 If Sensitive Security Information is disclosed other than as authorized by this Order, the  
5 Party or person responsible for the unauthorized disclosure, and any other Party, person, firm or entity  
6 who is subject to this Order and learns of the unauthorized disclosure, shall immediately bring such  
7 disclosure to the attention of TSA.  
8

9 10.2 The Party or person responsible for the unauthorized disclosure shall make every effort to  
10 obtain the return of the Sensitive Security Information (including, without limitation, from the person to  
11 whom the unauthorized disclosure was made and from any other person to whom Sensitive Security  
12 Information was transmitted as a direct or indirect result of the unauthorized disclosure) and to prevent  
13 further disclosure on its own part or on the part of any person to whom the unauthorized disclosure was  
14 made.  
15

16 10.3 In addition to any other remedies that are available under law, any Party, person, firm or  
17 entity responsible for an unauthorized disclosure of Sensitive Security Information protected by this  
18 Order may be subject to all remedies provided under 49 C.F.R. § 1520.17 and the Act.  
19

20 10.4 In the event that TSA determines that any Court Designated Covered Person has  
21 intentionally, willfully or recklessly disclosed Sensitive Security Information in violation of this Order,  
22 TSA may, in the exercise of its sole discretion, revoke such Court Designated Covered Person's  
23 clearance for access to Sensitive Security Information. Furthermore, TSA may consider such  
24 intentional, willful or reckless disclosure in determining whether granting access to Sensitive Security  
25 Information to any member of a firm or entity that employed such Court Designated Covered Person.  
26  
27  
28

1 **11. Reservation of Rights**

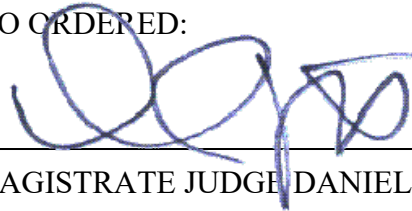
2 11.1 In the event that TSA determines that a Document containing Sensitive Security  
3 Information, or portion thereof, was inappropriately made available to the Parties, TSA reserves the  
4 right to remove the Document, or portion thereof, from this Litigation, and to take any other measures  
5 necessary to protect the Sensitive Security Information at issue.  
6

7 11.2 TSA reserves the right to revoke a Court Designated Covered Person's clearance in the  
8 event TSA obtains information that leads TSA to determine that granting such Court Designated  
9 Covered Person access to Sensitive Security Information presents a risk of harm to the nation.  
10

11 11.3. If it comes to TSA's attention that information or items that it designated as Sensitive  
12 Security Information do not qualify as Sensitive Security Information or have ceased to qualify as  
13 Sensitive Security Information, TSA will promptly notify all parties that it is withdrawing its Sensitive  
14 Security Information designation.

15 11.4 This Order is without prejudice to the rights of any party or government agency to make  
16 any claim of privilege or to make any objection to discovery or use of Sensitive Security Information, or  
17 documents that may contain Sensitive Security Information, permitted by the Federal Rules of Civil  
18 Procedure, or any other statute, regulation, or authority.  
19

20 IT IS SO ORDERED:

21   
22

23 U.S. MAGISTRATE JUDGE DANIEL J. ALBREGTS

24 Dated: July 16, 2021

1 /s/ John D. McKay

2 John D. McKay (admitted *pro hac vice*)  
3 PARK AVENUE LAW LLC  
4 127 West Fairbanks Avenue, Suite 519  
5 Winter Park, Florida 32789  
6 Phone: (800) 391-3654  
7 Email: [johndmckayatty@gmail.com](mailto:johndmckayatty@gmail.com)

8 Timothy R. Titolo (Nevada Bar No. 3617)  
9 TITOLO LAW OFFICE  
10 9950 West Cheyenne Avenue  
11 Las Vegas, Nevada  
12 Phone: (702) 869-51  
13 Email: [tim@titololaw.com](mailto:tim@titololaw.com)

14 *Attorneys for Plaintiffs*

/s/ Brian T. Maye

Brian T. Maye (admitted *pro hac vice*)  
Matthew D. Martin (admitted *pro hac vice*)  
ADLER MURPHY & McQUILLEN LLP  
20 South Clark Street, Suite 2500  
Chicago, Illinois 60603  
Email: [bmaye@amm-law.com](mailto:bmaye@amm-law.com)  
[mmartin@amm-law.com](mailto:mmartin@amm-law.com)

Charles A. Michalek (Nevada Bar No. 5721)  
ROGERS, MASTRANGELO, CARVALHO &  
MITCHELL  
700 South Third Street  
Las Vegas, Nevada 89101  
Phone: (702) 383-3400  
Email: [cmichalek@rmcmlaw.com](mailto:cmichalek@rmcmlaw.com)

*Attorneys for Defendants*

**EXHIBIT A**

**Agreement to Abide by the Terms of the Stipulated Protective Order Governing Access to, Handling of, and Disposition of Potential Sensitive Security Information in the matter of *DELVECCHIA V. FRONTIER AIRLINES*, 19-cv-01322, U.S. District Court for District of Nevada.**

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as set forth in the Stipulated Protective Order Governing Access to, Handling of, and Disposition of Potential Sensitive Security Information *DELVECCHIA V. FRONTIER AIRLINES*, 19-cv-01322, U.S. District Court for District of Nevada.

I make this Agreement in good faith, without mental reservation or purpose of evasion.

---

Print Name

---

Address

---

Telephone Number

---

Signature:

**WITNESS:**

---

Print Name

---

Address

---

Telephone Number

---

Signature: